The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

A. JOSEPH DeNUCCI
AUDITOR

No. 2002-0191-4C

INDEPENDENT STATE AUDITOR'S
REPORT ON EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AND THE BILLING AND RECEIVABLE SYSTEM AT BRISTOL COMMUNITY COLLEGE

September 1, 2000 through December 14, 2001

OFFICIAL AUDIT REPORT
FEBRUARY 28, 2002

TABLE OF CONTENTS

INTRODUCTION

Bristol Community College (BCC), which was established in 1965, is a two-year public community college with approximately 3,341 students in day programs and 2,342 students in continuing education evening courses. In addition, 4,000 students are enrolled in non-credit-earning courses, such as basic education or training programs, which are provided by the Division of Continuing Education and Community Services (now known as the Division of Enrollment, Workforce and Community Development). The campus is located on Elsbree Street in Fall River, however continuing education courses are also provided at satellite centers located in Attleboro, New Bedford, and Taunton. The College, which provides instruction and training in a variety of fields of study such as liberal arts and science, allied health, engineering technologies, and business, has been accredited by the New England Association of Schools and Colleges.

The College is heavily dependent on information technology to carry out its mission and education programs. BCC's information technology infrastructure has grown to encompass a variety of educational and administrative uses. Technology, including desktop support, administrative systems, and the telephone and network infrastructure is administered through the College's Information Technology Services (ITS), formerly Administrative Computing and Information Services.

The College's primary application system is the Banner administrative system that is used to support admissions, day and evening student records, financial aid, human resources, and financial records. The Banner application, which operates on a Sun Microsystems server using a Solaris platform as its operating system, is a fully integrated student and administrative system. The College's other file servers operate Windows NT and are used for electronic mail, printing, file sharing, and web-based services. The College uses WebCT software for its distance learning courses and is a member of the statewide distance-learning consortium.

The College's communication backbone consists primarily of multi-node fiber-optic cabling among its nine distinct buildings, with copper cabling within each building. The College has an Ethernet-based local area network (LAN) and is connected to the Internet through the University of Massachusetts with its connection point being the University of Massachusetts-Dartmouth campus. The College's New Bedford campus is connected to the main campus using two T1 leased telephone lines, one that is used for voice communications and the other for data transmission.

Campus users have other external available resources, including the library network, the Commonwealth’s Human Resources/Compensation Management System (HR/CMS), the State’s Information Warehouse, the Board of Higher Education’s Information Resource System (HEIRS), and the Massachusetts Management Accounting and Reporting System (MMARS).

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

Our audit, which was conducted from September 9, 2001 through December 14, 2001, covering the period of September 1, 2000 through December 14, 2001, consisted of an examination of selected controls related to the information technology (IT) processing environment at Bristol Community College (BCC). Our audit scope included an examination of IT-related controls pertaining to organization and management, physical security and environmental protection of IT equipment in the computer room and selected sites housing IT resources throughout the College, system access security for data operations and systems residing on file servers, disaster recovery and business continuity planning for IT-related services, on-site and off-site storage of backup magnetic media, and user satisfaction regarding services provided by ITS. In addition, we reviewed the Banner application, a software system that the College uses to record and track student records, financial records and human resource information.

Audit Objectives

Our primary objective was to determine whether selected IT-related controls were in place and in effect within the College's IT processing environment. In this regard, we sought to determine whether the College's IT-related internal control environment, including policies, procedures, practices, and organizational structure provided reasonable assurance that control objectives would be achieved to support business functions to determine whether IT-related assets were adequately safeguarded from damage or loss. We sought to determine whether adequate physical security and environmental protection controls were in place over IT operations. We also sought to determine whether adequate controls were in place to prevent and detect unauthorized system access to the data files and software residing on the servers and BCC's microcomputer systems. Regarding system availability, we sought to determine whether adequate business continuity plans were in effect to provide reasonable assurance that mission-critical and essential systems could be regained within an acceptable period of time should a disaster render processing inoperable. Moreover, we determined whether adequate on-site and off-site storage was being provided for backup copies of magnetic computer media and whether users were satisfied with the support being provided by ITS.

We sought to determine whether the data in the Banner software application remained complete, accurate, and valid during input, update, and storage. In conjunction with our review of payment information processed through the Banner application, we reviewed a sample of twenty-five student account-history files to verify whether refunds were made in accordance with BCC's collection refund policy.

Audit Methodology

To determine the scope of the audit, we performed a pre-audit survey regarding the College's IT environment. To determine the audit objectives, we conducted pre-audit work, which included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of IT-related internal controls, and interviewing senior management to discuss the College's control environment. We conducted site visits to the BCC computer room and selected sites housing microcomputers. We performed a risk analysis of IT operations and selected applications in order to select areas to be tested. To assess the adequacy of selected internal controls regarding IT and selected application operations, we interviewed management and staff, observed operations, and performed selected audit tests.

Regarding our review of organization and management, we interviewed senior management, reviewed the College's organizational structure with respect to IT operations, reviewed and analyzed IT policy and procedure documentation, and assessed IT-related general controls and practices. To determine whether IT-related assets were adequately safeguarded from damage or loss, we reviewed physical security and environmental protection over computer operations through observation, completing appropriate checklists, and conducting interviews with BCC staff.

To obtain an understanding of access security controls, we reviewed the College's system access security policies and procedures designed to prevent and detect unauthorized access to the data files and applications on the College's file servers and microcomputer systems. To determine whether system access security was being properly maintained through the management of user IDs, passwords and user access privilege profiles, we interviewed the security administrator and assessed the level of access security being provided. To determine whether access privileges of BCC's employees authorized to access the file servers and microcomputer systems were properly authorized and consistent with job responsibilities and functions, we reviewed procedures for granting system access and user profile administration. We determined whether procedures were in place to ensure that the security administrator was promptly and properly notified of a change in personnel status (e.g., employment termination, job transfer, or leave of absence) so that user IDs and passwords could be promptly deactivated from the system or the access privileges be appropriately modified. We obtained a list of authorized users from the security administrator and a list of current employees from BCC's Human Resources department and compared them to verify that all of the authorized users were current employees.

To assess the adequacy of disaster recovery and business continuity planning, we reviewed the nature and extent of documented policies, procedures, and practices used to resume computer operations in a timely manner should automated systems be damaged, destroyed, or rendered inoperable. To evaluate the adequacy of controls to protect file servers and microcomputer-based data files and software, we interviewed management at BCC and reviewed the current business continuity plan against established industry standards. Further, we interviewed management and staff and assessed the frequency of transfer of copies of backup media and maintenance of backup logs for on-site storage. We also assessed the physical security and environmental protection for the on-site storage area. The College had a contracted vendor to store weekly backup copies of magnetic media; however, we did not visit the off-site storage facility.

To evaluate the Banner application software and to obtain and record an understanding of the procedures used to record and update student payment information, we interviewed senior management of the BCC's Comptroller and Bursar's Office. We reviewed relevant policies and procedures for collecting, recording, and depositing cash receipts. In addition, we interviewed personnel in the Accounting Department in order to obtain an understanding of the process of recording cash receipts in the College's financial records for the academic year of September 1, 2000 through June 30, 2001. To test billing and receivable records, we judgmentally sampled all transactions on four of twenty-one business days in the month of January 2001. We compared a sample of billing and receivable records produced by the automated system to actual student records by tracing individual transactions recorded in cashier-session reports from the time of receipt through the formal recording in the College's Accounting Department records. In addition, we reviewed daily batches, bank deposit receipts, armored-car receipts, credit card receipts, cash receipt entry logs, daily on-line transcript reports, weekly reports, bank reconciliations, and student account-history files. We verified selected daily transactions from the cash collection process to student account-history files by comparing source documents to information contained in reports that were generated by the automated system. In addition, we verified selected cash receipts to bank deposit slips and bank reconciliation reports and credit card receipts to batch reports and bank records.   We also traced selected student refunds from the College’s check register to student account-history files in order to verify whether refunds made were in accordance with BCC’s collection refund policy.

To determine whether users were satisfied with the support provided by the ITS, we interviewed selected users regarding ease of system use, continuous access to necessary applications, and system-related problem resolution, as applicable.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and industry auditing practices.

AUDIT SUMMARY

Based on our audit at Bristol Community College, we found that internal controls in place provided reasonable assurance that IT-related control objectives regarding organization and management, physical security, environmental protection, business continuity planning, and on-site and off-site storage of magnetic media would be met. Although we found controls to be generally adequate in the area of system access security, certain policies and procedures should be strengthened to provide reasonable assurance that only authorized access can be gained to the College's administrative systems. With respect to our tests of data integrity of student payment information controlled through the Banner application software, our tests of source documents indicated that for the selected transactions, the data remained complete, accurate, and valid during the stages of input, update, and storage.

Our review of the BCC's organization and management over IT-related activities disclosed that organizational controls were in place and that documented policies, procedures, and practices existed and were adequate. Further, regarding IT-related organization and management, we found that there were sufficient controls in place with respect to reporting lines, segregation of duties, span of control, and oversight.

Regarding physical security, we determined that access control over the computer room was adequate to safeguard entrance to the facility. However, we suggested that the College consider installing an intrusion alarm on the door to further strengthen physical security controls. The College agreed with our recommendation and was in the process of installing an intrusion detection alarm to improve physical security over the IT-related resources in the computer room. We found that environmental protection controls were in place in the computer room for fire suppression, temperature and humidity control, and smoke detection. In addition, to help ensure uninterrupted computer operations and data integrity, BCC maintains two uninterruptible power supply (UPS) units in the computer room, as well as additional UPS units on other servers throughout the campus. The UPS units provide protection against power spikes and brownouts and allow the equipment to be powered down in a logical sequence, without potential damage to data files or IT resources, given a sudden loss of electrical power.

We found that appropriate procedures were in effect for generating backup copies of magnetic media and for storing the backup tapes on-site, as well as at a contracted off-site location. We further determined that the storage facility housing on-site backup copies of computer-related media was adequately safeguarded and environmentally protected. However, we did not inspect the off-site storage location. Regarding system availability, we also found that Information Technology Services (ITS) had developed a comprehensive business continuity plan that outlined a sound strategy for maintaining system availability in the event of a major disaster or disruption of IT operations. In addition, the plan had been recently updated during our audit period.

Based on our review of system access security, BCC's policies and procedures appeared to provide reasonable assurance that only authorized users had access to applications and workstations connected through the local area network. We also found BCC's controls over the administration of user IDs and passwords to be adequate. Although documented policies and control practices provided reasonable assurance that access privileges would be deactivated or appropriately modified in a timely manner should individuals having access terminate employment or incur a change in job requirements, the results of our tests indicated that user IDs and passwords for three former BCC employees had not been removed for up to four months from the time they left because a "Computer Access Request Form" had not been completed and forwarded to the security administrator. Based on our analysis of a completed questionnaire with selected users, we found that the users were satisfied with the support received from ITS and that users had continuous access to system resources.

Based on tests performed with respect to data integrity for transactions processed through the Banner application, by comparisons to source documents, we verified that data remained complete, accurate, and valid during input, update, and storage. Specifically, our tests indicated that there were adequate controls in place to ensure that student-payment information was accurately recorded and verified for the selected test of transactions, not only on the College's summary reports, but also on the students' individual account records. In addition, our tests indicated that the selected refunds tested for the Spring 2001 semester were accurately made in accordance with the BCC refund policy.

AUDIT RESULT

System Access Security

We found that, although BCC's policies and procedures in regard to access to data files and software provided reasonable assurance that access privileges would be deactivated or appropriately modified in a timely manner should individuals' access requirement circumstances change, they were not always being followed. We determined that controls needed to be strengthened to ensure that logon user IDs and passwords would be revoked for individuals no longer authorized or needing access to automated systems. We also found that, although ITS had a form for the deactivation of users, the security administrator was not being notified in a timely manner when access requirements changed so that access could be modified or deactivated in a timely manner.

We determined that notifications of terminations were generally made to the security administrator. BCC's user account policy states, "If an employee leaves the College, the supervisor forwards a copy of the *Computer Access Request Form* and indicates that the employee has left the College and when access should be terminated." However, we found that logon user IDs and passwords were still active for three former BCC employees who had left the employment of the College as far back as four months prior to our audit. It appeared that the access privileges had not been deactivated because the security administrator had not been notified of the changes in employment status. Changes in employment, such as extended leaves of absence, changes in responsibilities, or terminations of employment that could impact authorized system access should be reported immediately to the system security administrator to enable timely deactivation of logon user IDs and passwords or the modification of access privileges to reflect the changes in employment responsibilities.

Without timely deactivation of user IDs and passwords, BCC's data are susceptible to unauthorized use, disclosure, or loss. Computer industry standards indicated that access to information system workstations and data should be restricted to specific users to prevent and detect unauthorized system access through the implementation of formal control procedures.

Recommendation:

We recommend that the security administrator, in conjunction with BCC's Human Resources Department, develop appropriate monitoring procedures to ensure adherence to the current user account policy. As required by the computer access request form, timely notification of employee terminations should be forwarded to the security administrator so that access can be deactivated in a timely manner. We also recommend that the form be modified to include a requirement that changes in job responsibilities requiring changes in access privileges also promptly be reported to the security administrator to allow for timely modification of access privileges.

Auditee's Response:

> *We concur with the audit finding regarding departed employee system access and have altered our procedures to ensure that the College's security administrator is notified immediately upon an employee's departure.*

Auditor's Reply:

We concur with the College's actions initiated to strengthen access security controls. We will review these control enhancements during our next IT audit.